Prof. Philip Koopman

Carnegie Mellon University

Driver Assistance vs. Automated Vehicle Safety

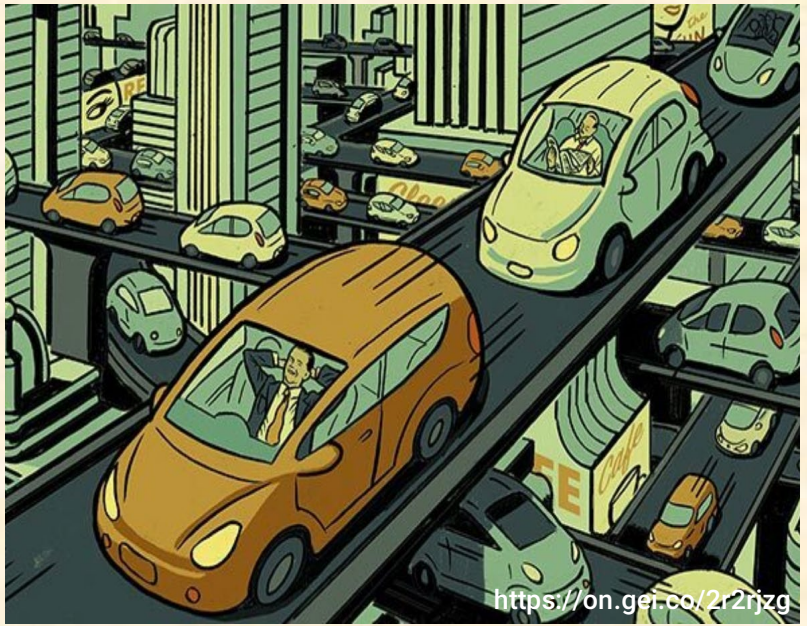
ISSC / August 18, 2021

@PhilKoopman

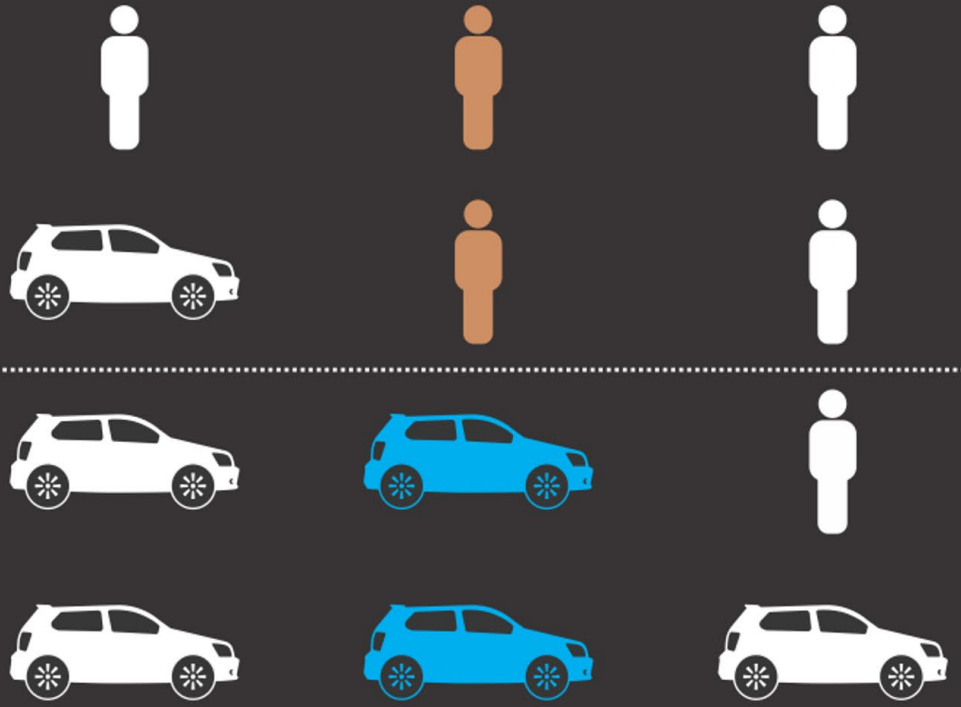
Overview

Carnegie Mellon University

- Driver Assistance:
  - Help human drivers be better & safer
- Driver Automation:
  - Vehicle actually drives
- Compare & contrast
  - Safety argument implications
  - Technology challenges
- Start with:
  - Automation modes for non-engineers



Operating Mode	Human Role	Driving	Driving Safety	Other Safety	
Assistive	Driving				Driver Assistance
Supervised	Eyes ON the road				
Automated	Eyes OFF the road				Automated Driving
Autonomous	No human				



Vehicle Automation Modes

https://bit.ly/3r1dhKE

Assistive: Help the Driver Drive

Carnegie Mellon University

- Better execute driver commands
  - Anti-lock brakes
  - Electronic stability control
- Momentarily intervene for safety
  - Automated emergency braking

- The driver is responsible for safety
  - The vehicle obeys driver intent
  - Interventions to improve driver performance
  - Functional safety covers equipment failures (ISO 26262)

Supervised: Driver Monitors for Safety

Carnegie Mellon University

- Vehicle (mostly) does the driving
  - Speed control & lane keeping
- Human driver responsible for safety
  - Intervene to handle edge cases

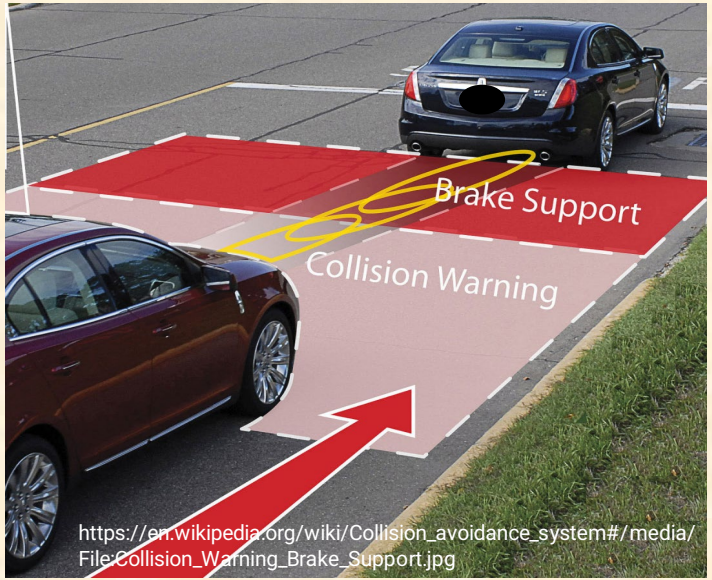
Shutterstock/Metamorworks

- Driver monitors and intervenes
  - Vehicle must let driver intervene when needed (ISO 26262)
  - Effective driver monitoring required for automation complacency
  - Safety Of The Intended Function (SOTIF) (ISO 21448) helpful

ADAS Safety – Helping the Driver

Carnegie Mellon University

- Proper functionality helps driver
  - Reduce driver stress, control mistakes
- Active safety can help
  - Helps avoid crashes
  - Tune to avoid false activations
- Arguably, good enough active safety
  - ADAS claims credit for safety; human blamed for crashes
  - BUT: avoid unreasonable demands on human drivers
    - Unaided humans are terrible at monitoring boring automation



https://en.wikipedia.org/wiki/Collision_avoidance_system#/media/File:Collision_Warning_Brake_Support.jpg

Automated: The Car Drives

Carnegie Mellon University

- Vehicle drives & handles safety
  - Driver need not pay attention to driving
  - Driving problems *not* dumped onto driver
- The vehicle responsible for driving safety
  - By definition:
    collisions are not fault of a human driver
- Tension between safety and permissiveness
  - False non-detections (false negatives) generally hurt safety
  - False detections (false positives) generally hurt permissiveness

Autonomous: No Human Oversight

Carnegie Mellon University

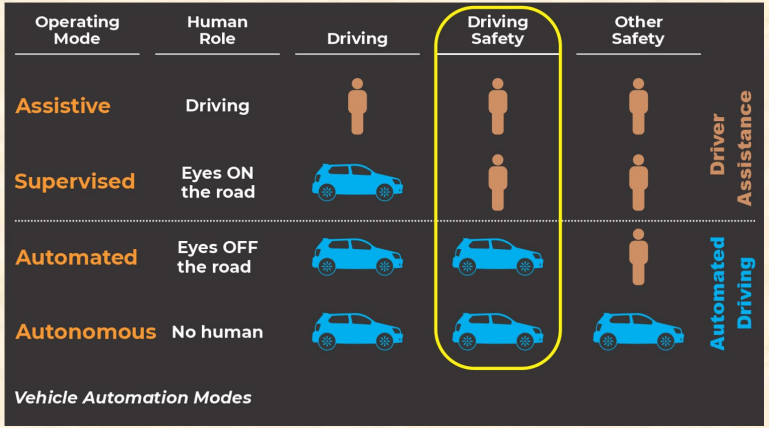
- Vehicle handles driving & vehicle safety
  - There is no driver; no human supervision
  - Ensures passenger & cargo safety
  - Handles non-driving issues (e.g., post-crash)

- The vehicle is responsible safe operation
  - Human does not help with safety
  - OK for vehicle to get help if it initiates request all on its own
- Adds requirement for non-driving sensing (UL 4600)
  - Passenger safety; cargo safety; vehicle equipment status
  - Beyond scope of Automated Driving System Levels in J3016

Driver Roles Contrasted

Carnegie Mellon University

- **Assistive & Supervised**
  - Driver attention required
  - Vehicle responds to driver
  - Vehicle blame for unsafe intervention
    - Incentive for vehicle to under-perform



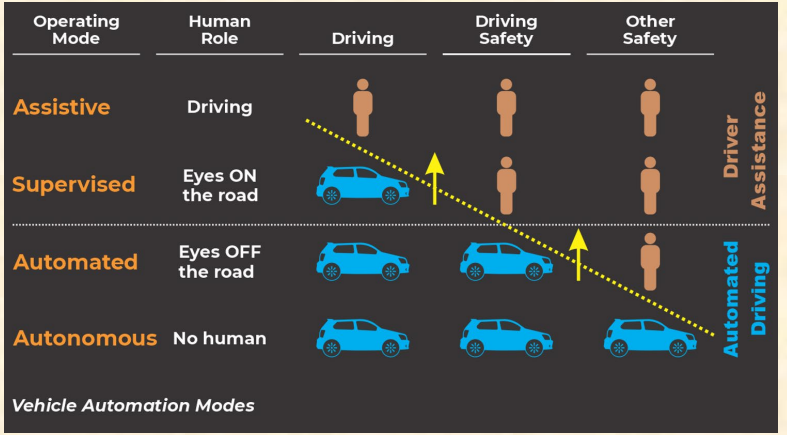
https://bit.ly/3r1dhKE

- **Automated & Autonomous**
  - No human attention on driving
    - Vehicle cannot count on human intervention for driving safety
  - Mode changes are requests, not demands by vehicle
    - Human actively confirms responsibility

Driver Mode Transitions

Carnegie Mellon University

- Mode confusion is a problem
  - Driver positive acknowledgment
  - Request user attention, not “demand”
- Example issues:
  - Supervised changes to Assistive
    - Driver thinks vehicle is still steering
  - Automated changes to Supervised
    - Driver takes extended time to regain situational awareness
    - “Captain of ship” does not have a full driving license
  - Autonomous changes to Automated
    - Attendant rouses then falls back asleep (sleeps through alarm)

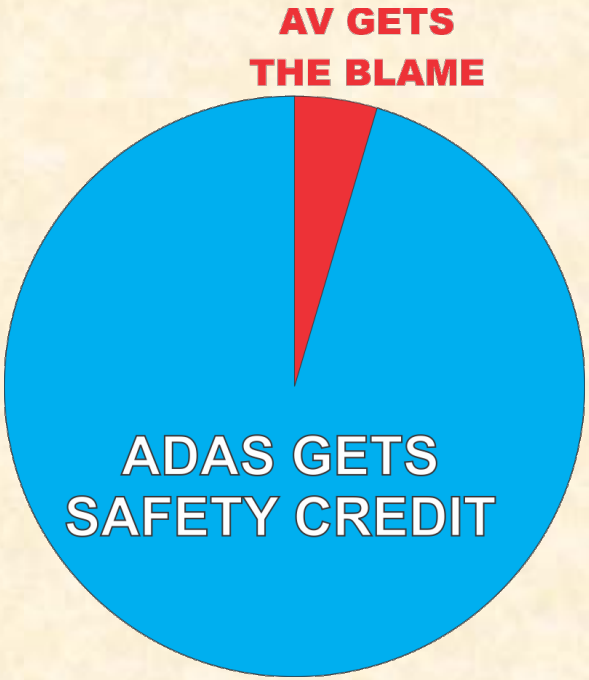


https://bit.ly/3r1dhKE

Automation Safety Challenges

Carnegie Mellon University

- Assistive
  - More uniform adoption of ISO 26262
- Supervised
  - Safety credit if low false positives
  - Effective driver monitoring
- Automated
  - SOTIF, scenario completeness & coverage
  - Sensor fusion, perception, prediction
  - Blamed for false negatives
- Autonomous
  - UL 4600 coverage: drivers do more than drive



Component Safety Challenges

Carnegie Mellon University

- Positive Trust Balance:
  - Engineering Rigor, Validation, Feedback, Safety Culture
  - Standards-driven safety
- Safety Performance Indicators (SPIs)
  - Integrators asking for component safety cases
  - Field feedback: development; deployed
- Scalability past pilot vehicles
  - Accurate perception/prediction is still work in progress
  - Transition from brute force data to safety case
  - Key point: avoiding multi-sensor correlated failures

Organizational Safety Challenges

Carnegie Mellon University

- Significant pressure to deploy
  - Flurry of empty driver seat demos in 2020
  - Can teams take the time needed for safety?
- Industry transparency needed
  - Safety collaboration rather than competition
  - Public trust in face of an adverse news event
- Ensuring robust safety cultures
  - Robotics meets automotive engineering
  - Silicon Valley culture + automotive culture + no human driver

https://youtu.be/nhqyrze30bk
Yandex demo video, Ann Arbor, Aug 2020